[RENESAS SECURITY PROCESS INTRODUCTION TRAINING]

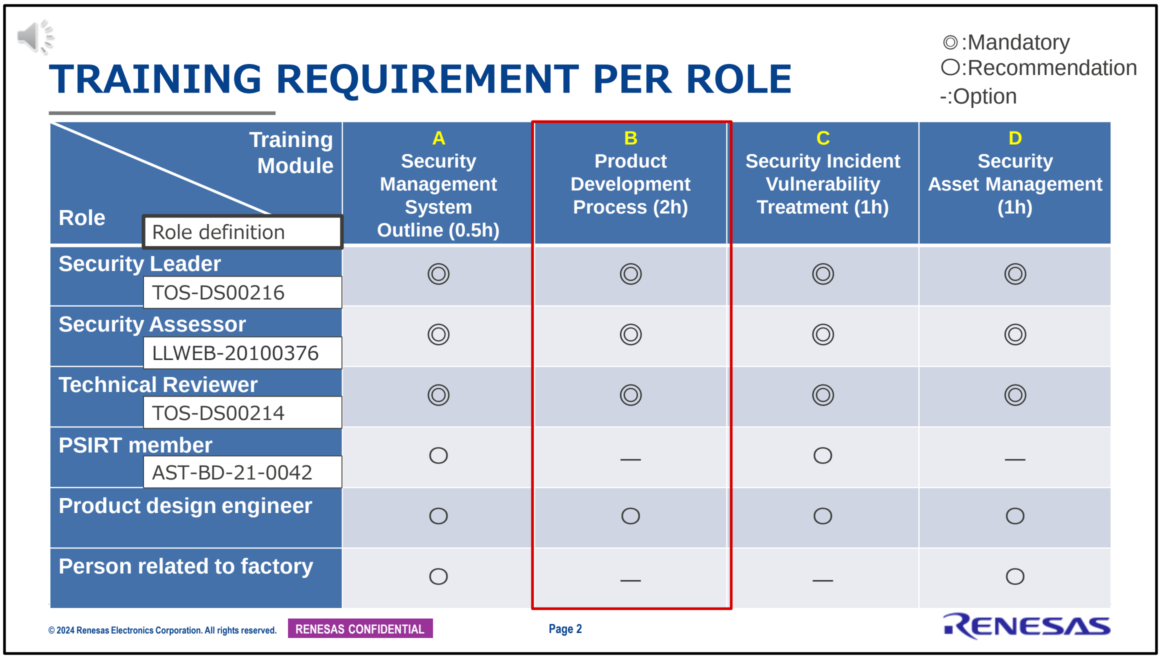
SECURITY PRODUCT DEVELOPMENT PROCESS FOR AUTOMOTIVE PRODUCTS

(REQUIREMENT MANAGEMENT PROCESS / SEMICONDUCTOR PRODUCT DEVELOPMENT / SOFTWARE PRODUCT DEVELOPMENT)

REV.3.0 3RD JUN. 2024 REL/DO/QAD/QSP/QDSC S. NAGATA、 K. AMIMOTO, K. FUJII

RENESAS CONFIDENTIAL

This video is a lecture video on the requirements management process of the security product development process for automotive products.



TRAINING REQUIREMENT PER ROLE

◎:Mandatory
○:Recommendation
-:Option

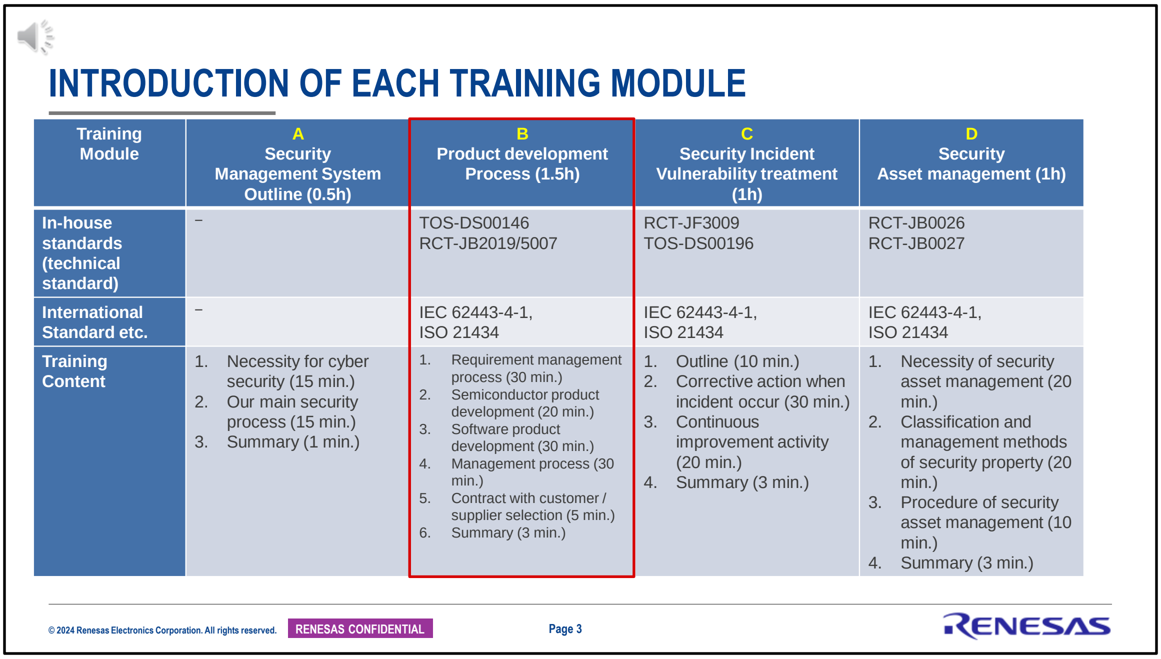
Training Module Role Role definition	A Security Management System Outline (0.5h)	B Product Development Process (2h)	C Security Incident Vulnerability Treatment (1h)	D Security Asset Management (1h)
Security Leader TOS-DS00216	◎	◎	◎	◎
Security Assessor LLWEB-20100376	◎	◎	◎	◎
Technical Reviewer TOS-DS00214	◎	◎	◎	◎
PSIRT member AST-BD-21-0042	○	—	○	—
Product design engineer	○	○	○	○
Person related to factory	○	—	—	○

RENESAS CONFIDENTIAL

Page 2

RENESAS

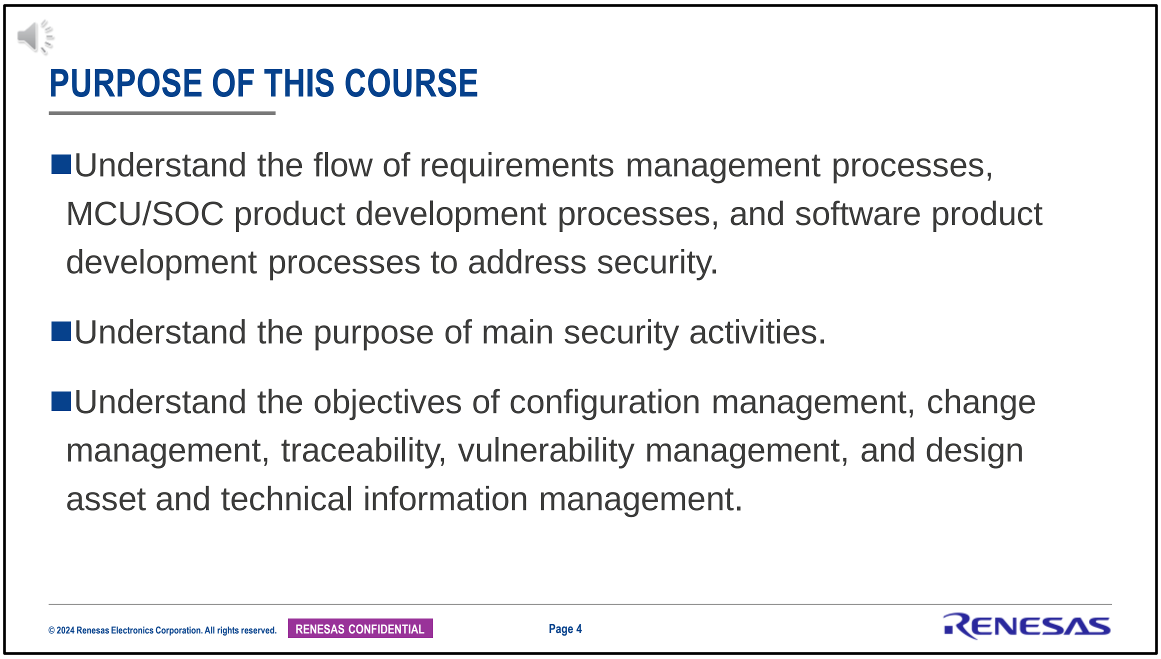
This is a table of participants for each training module.
We offer four training modules as security process introduction education.
The main roles in security-enabled development are security leaders, security assessors, technical reviewers, and PSIRT.
This table shows the training required for each role.
Double circles are mandatory, circles are recommendation, and bars are option.
Role definition have been established for each role, setting out certification and appointment procedures. It specifies the training required for certification.
This course, Product development process, is considered essential education for certification of security leaders, security assessors, and technical reviewers.



INTRODUCTION OF EACH TRAINING MODULE

Training Module	A Security Management System Outline (0.5h)	B Product development Process (1.5h)	C Security Incident Vulnerability treatment (1h)	D Security Asset management (1h)
In-house standards (technical standard)	–	TOS-DS00146 RCT-JB2019/5007	RCT-JF3009 TOS-DS00196	RCT-JB0026 RCT-JB0027
International Standard etc.	–	IEC 62443-4-1, ISO 21434	IEC 62443-4-1, ISO 21434	IEC 62443-4-1, ISO 21434
Training Content	1. Necessity for cyber security (15 min.) 2. Our main security process (15 min.) 3. Summary (1 min.)	1. Requirement management process (30 min.) 2. Semiconductor product development (20 min.) 3. Software product development (30 min.) 4. Management process (30 min.) 5. Contract with customer / supplier selection (5 min.) 6. Summary (3 min.)	1. Outline (10 min.) 2. Corrective action when incident occur (30 min.) 3. Continuous improvement activity (20 min.) 4. Summary (3 min.)	1. Necessity of security asset management (20 min.) 2. Classification and management methods of security property (20 min.) 3. Procedure of security asset management (10 min.) 4. Summary (3 min.)

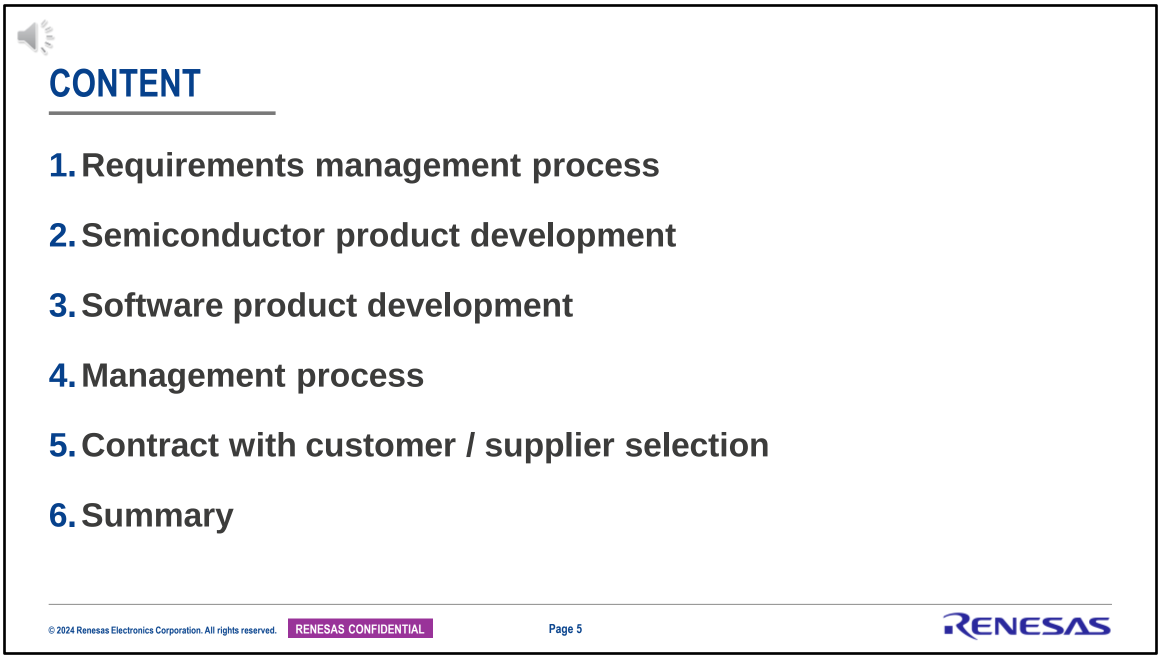
An introduction of each training module.
It shows related in-house standards, international standards, and the content of each training.
This course is designed to explain the development process of security-enabled products.
Describes requirements management processes, semiconductor product development, software product development, and management processes such as configuration management and change management. The total length is 1 hour and 30 minutes.



PURPOSE OF THIS COURSE

- Understand the flow of requirements management processes, MCU/SOC product development processes, and software product development processes to address security.
- Understand the purpose of main security activities.
- Understand the objectives of configuration management, change management, traceability, vulnerability management, and design asset and technical information management.

This is the purpose of this course. There are three.
The first is to understand the flow of requirements management processes, MCU/SOC product development processes, and software product development processes to address security.
The second is to understand the purpose of main security activities.
The third is to understand the objectives of configuration management, change management, traceability, vulnerability management, and design asset and technical information management.



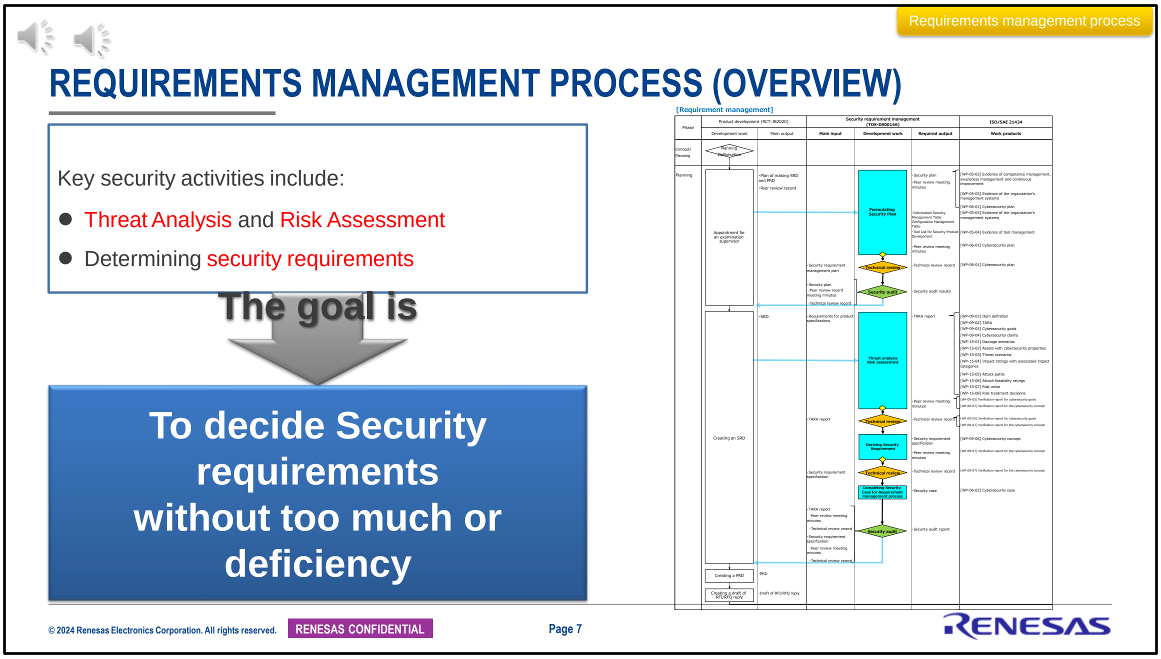
CONTENT

1. Requirements management process
2. Semiconductor product development
3. Software product development
4. Management process
5. Contract with customer / supplier selection
6. Summary

This is the content of this course.
1, Requirements management process
2, Semiconductor product development
3, Software product development
4, Management process
5, Contract with customer / supplier selection
6, Summary

1. REQUIREMENTS MANAGEMENT PROCESS

1, Requirements management process.
From here, we will explain the security activities carried out during the requirements management process in accordance with TOS-DS00146 Automotive Security product development Requirements Management Guidelines.



Requirements management process

REQUIREMENTS MANAGEMENT PROCESS (OVERVIEW)

Key security activities include:

- Threat Analysis and Risk Assessment
- Determining security requirements

The goal is

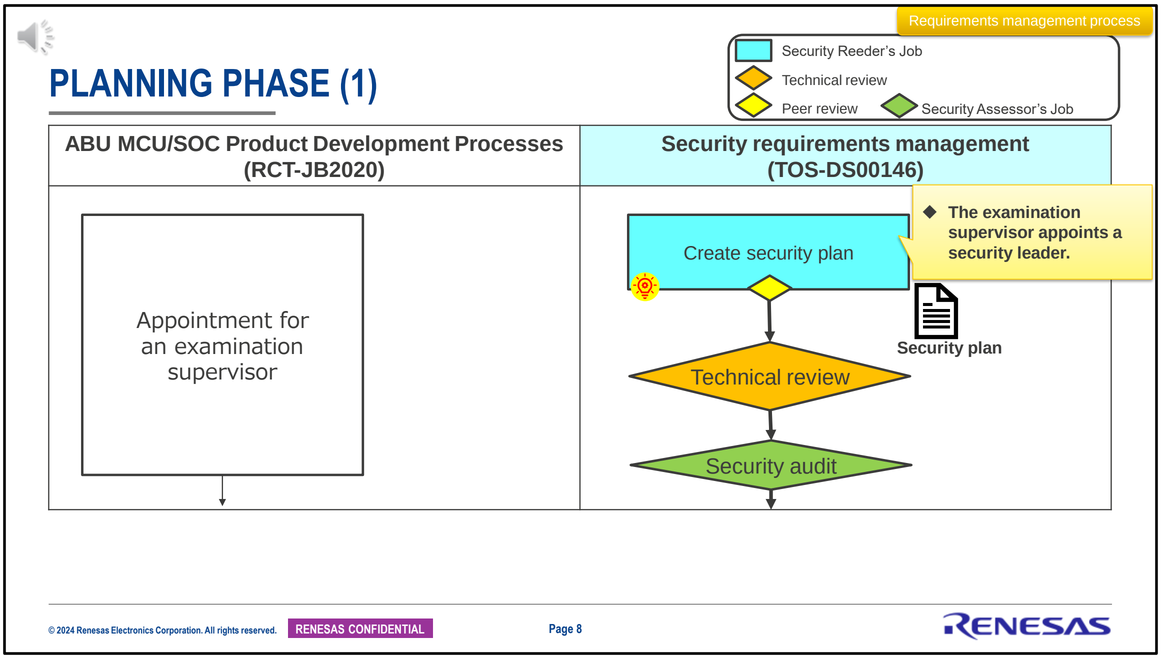
To decide Security requirements without too much or deficiency

[Requirement management]
Phase
Product development (RCT-JB2020)
Development work
Main output
Security requirement management (TOS-DS00146)
Main input
Development work
Required output
ISO/SAE 21434
Work products
Concept/ Planning
Planning Deliberation
Planning
Appointment for an examination supervisor
・Plan of making SRD and PRD
・Peer review record
Formulating Security Plan
・Security plan
・Peer review meeting minutes
[WP-05-02] Evidence of competence management, awareness management and continuous improvement
[WP-05-03] Evidence of the organization's management systems
[WP-06-01] Cybersecurity plan
・Information Security Management Table Configuration Management Table
[WP-05-03] Evidence of the organization's management systems
・Tool List for Security Product Development
[WP-05-04] Evidence of tool management
・Peer review meeting minutes
[WP-06-01] Cybersecurity plan
・Security requirement management plan
Technical review
・Technical review record
[WP-06-01] Cybersecurity plan
・Security plan
・Peer review record meeting minutes
・Technical review record
Security audit
・Security audit results
Creating an SRD
・SRD
・Requirements for product specifications
Threat analysis Risk assessment
・TARA report
[WP-09-01] Item definition
[WP-09-02] TARA
[WP-09-03] Cybersecurity goals
[WP-09-04] Cybersecurity claims
[WP-15-01] Damage scenarios
[WP-15-02] Assets with cybersecurity properties
[WP-15-03] Threat scenarios
[WP-15-04] Impact ratings with associated impact categories
[WP-15-05] Attack paths
[WP-15-06] Attach feasibility ratings
[WP-15-07] Risk value
[WP-15-08] Risk treatment decisions
・Peer review meeting minutes
[WP-09-05] Verification report for cybersecurity goals
[WP-09-07] Verification report for the cybersecurity concept
・TARA report
Technical review
・Technical review record
[WP-09-05] Verification report for cybersecurity goals
[WP-09-07] Verification report for the cybersecurity concept
Deriving Security Requirement
・Security requirement specification
[WP-09-06] Cybersecurity concept
・Peer review meeting minutes
[WP-09-07] Verification report for the cybersecurity concept
・Security requirement specification
Technical review
・Technical review record
[WP-09-07] Verification report for the cybersecurity concept
Completing Security Case for Requirement management process
・Security case
[WP-06-02] Cybersecurity case
・TARA report
・Peer review meeting minutes
・Technical review record
・Security requirement specification
・Peer review meeting minutes
・Technical review record
Security audit
・Security audit report
Creating a PRD
・PRD
Creating a draft of RFI/RFQ reply
・Draft of RFI/RFQ reply

RENESAS CONFIDENTIAL

Requirements management process (overview)
On the right is a security colorful chart for the requirements management process.
Although it is a bit small and difficult to see, the light blue squares indicate security activities added for security measures, and the orange diamonds indicate technical reviews. The green diamond is a security audit.
The main activities of the security requirements management process are performing threat analysis and risk assessment, and determining security requirements specifications.
The goal of these activities is to determine just the right amount of security requirements.

From the next page, we will explain the security development process while comparing it to QM's development process.



Requirements management process

PLANNING PHASE (1)

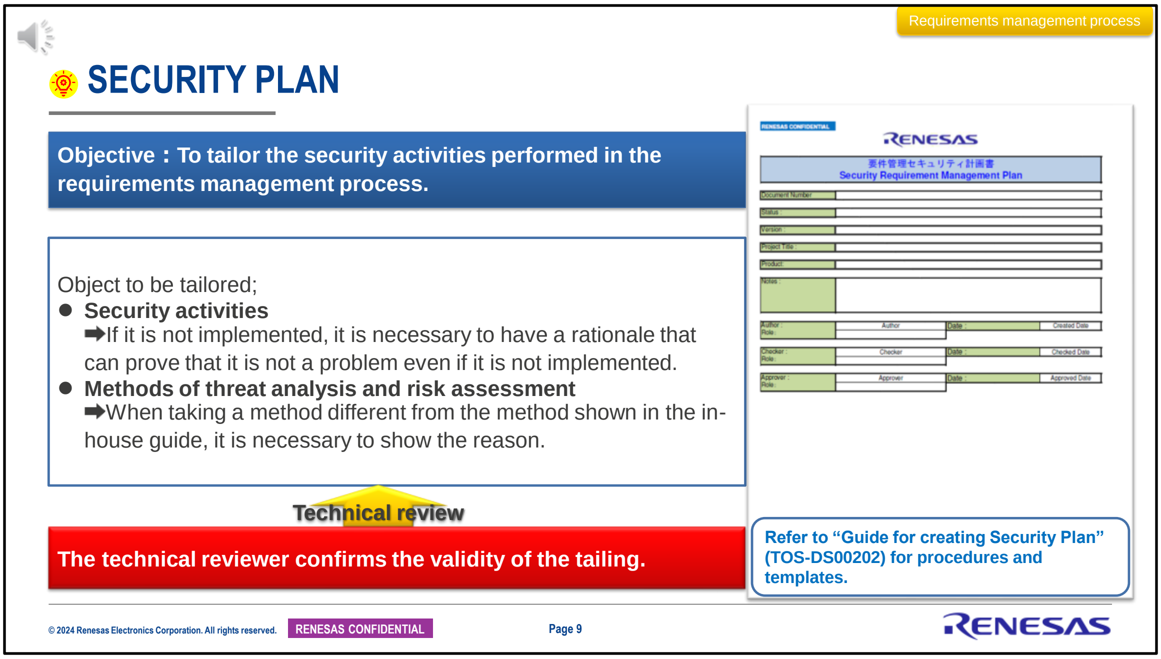
🟦 Security Reeder's Job
◆ Technical review
◆ Peer review ◆ Security Assessor's Job

ABU MCU/SOC Product Development Processes (RCT-JB2020)	Security requirements management (TOS-DS00146)
Appointment for an examination supervisor	Create security plan Technical review Security audit Security plan

- The examination supervisor appoints a security leader.

RENESAS CONFIDENTIAL

This is the planning phase.
On the left is the development process of the QM standard RCT-JB2020, and on the right is the development flow of TOS-DS00146, which defines security activities.
A security plan, which is a plan for security activities, is developed at the time when the examination supervisor is appointed in accordance with RCT-JB2020. This security plan is created by security leader. The development of a security plan begins when the examination supervisor appointed during QM development appoints a security leader.
The security plan is explained on the next page.
The created security plan is peer reviewed and then reviewed by technical reviewers. After the technical review has completed the resolution of the findings, a security assessor conducts a security audit.



Requirements management process

SECURITY PLAN

Objective：To tailor the security activities performed in the requirements management process.

Object to be tailored;

- **Security activities**
  ➡If it is not implemented, it is necessary to have a rationale that can prove that it is not a problem even if it is not implemented.
- **Methods of threat analysis and risk assessment**
  ➡When taking a method different from the method shown in the in-house guide, it is necessary to show the reason.

Technical review

The technical reviewer confirms the validity of the tailing.

RENESAS CONFIDENTIAL

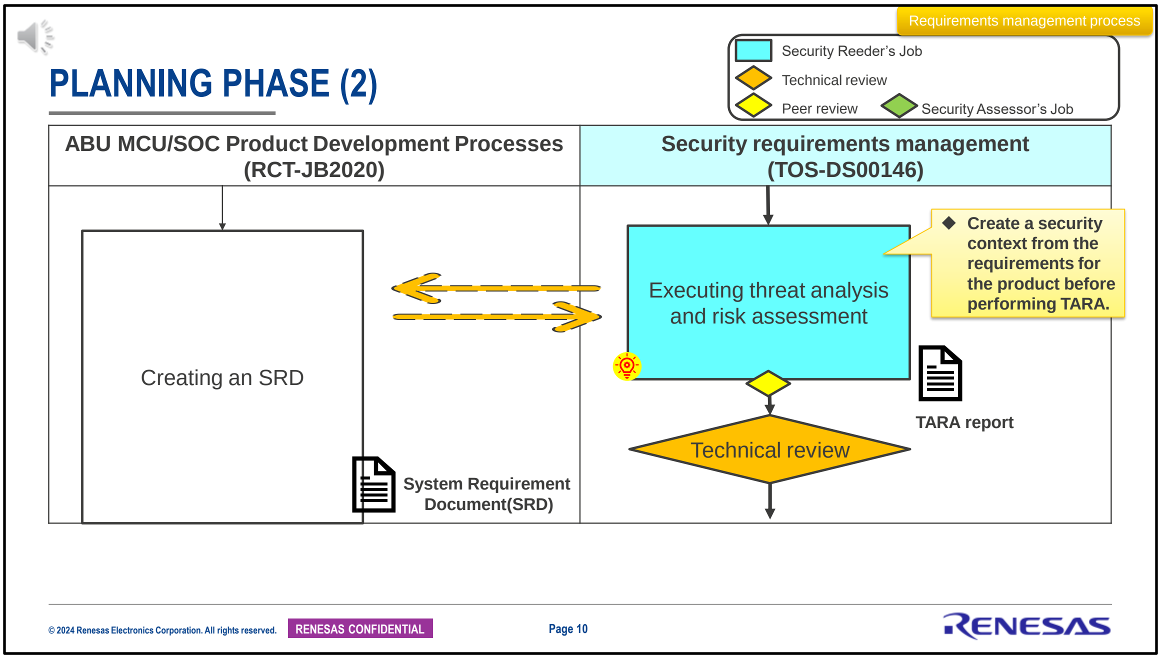
RENESAS

要件管理セキュリティ計画書
Security Requirement Management Plan

Document Number			
Status :			
Version :			
Project Title :			
Product:			
Notes :			
Author : Role :	Author	Date :	Created Date
Checker : Role :	Checker	Date :	Checked Date
Approver : Role :	Approver	Date :	Approved Date

Refer to "Guide for creating Security Plan" (TOS-DS00202) for procedures and templates.

Security plan.
The purpose of security planning is to tailor the security activities to be carried out in the requirements management process. One of the targets of tailoring is security activities. The other is the methods of threat analysis and risk assessment.
If the results of reuse analysis indicate that the product can be reused without changing the threat analysis risk assessment results, explain that there is no problem even if threat analysis risk assessment is not performed on the product. A logical basis is required. If you use a different method for threat analysis than the internal guide, you need to record the rationale. After a peer review of the security plan containing the results of these tailoring, a technical review is conducted by a technical reviewer to confirm the validity of the tailoring. Regarding the procedure and format for creating a security plan, I think that in most cases, you will follow internal guidelines, unless specified by the customer.
Please refer to our internal guide, TOS-DS00202 Security Plan Creation Guide.



Requirements management process

🟦 Security Reeder's Job
🔶 Technical review
◆ Peer review ◆ Security Assessor's Job

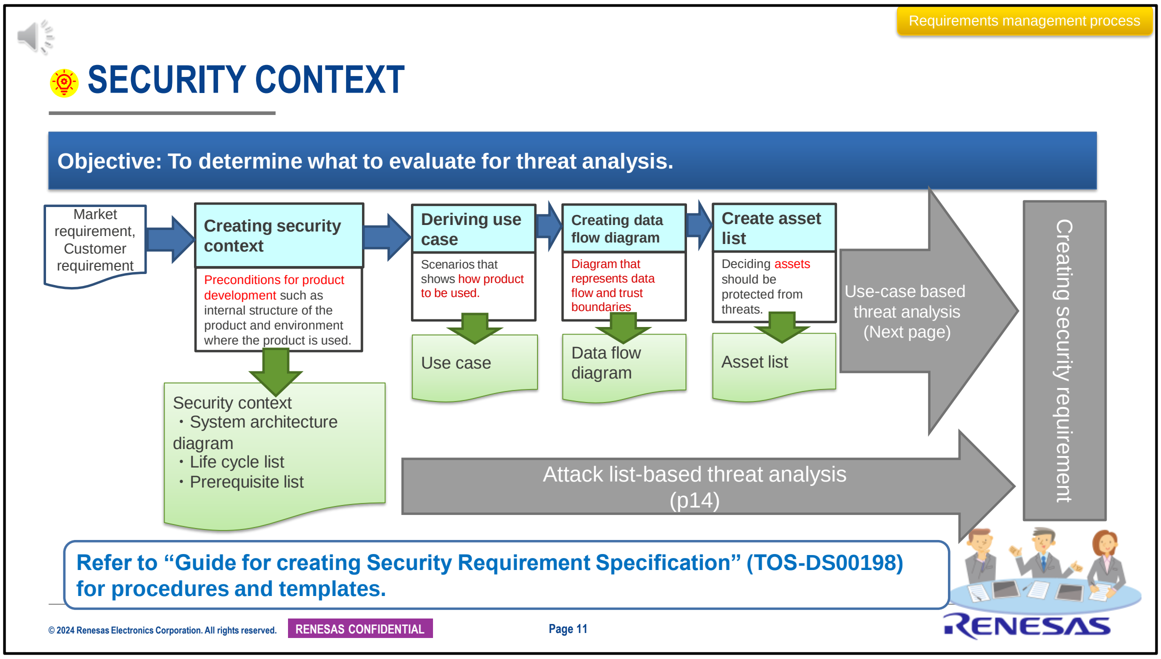
PLANNING PHASE (2)

ABU MCU/SOC Product Development Processes (RCT-JB2020)
Security requirements management (TOS-DS00146)
Creating an SRD
System Requirement Document(SRD)
Executing threat analysis and risk assessment
TARA report
Technical review

- Create a security context from the requirements for the product before performing TARA.

RENESAS CONFIDENTIAL Page 10 RENESAS

Also, let's go back to explaining the development flow.
A System Requirement Document, SRD, is created in accordance with RCT-JB2020. At the same time, security activities include creating a security context and conducting threat analysis and risk assessment.
A technical review is conducted on those results. This threat analysis and risk assessment, so we call it TARA, with the acronym T A R A.
Security context and threat analysis and risk assessment are discussed in the following pages.



Requirements management process

SECURITY CONTEXT

Objective: To determine what to evaluate for threat analysis.

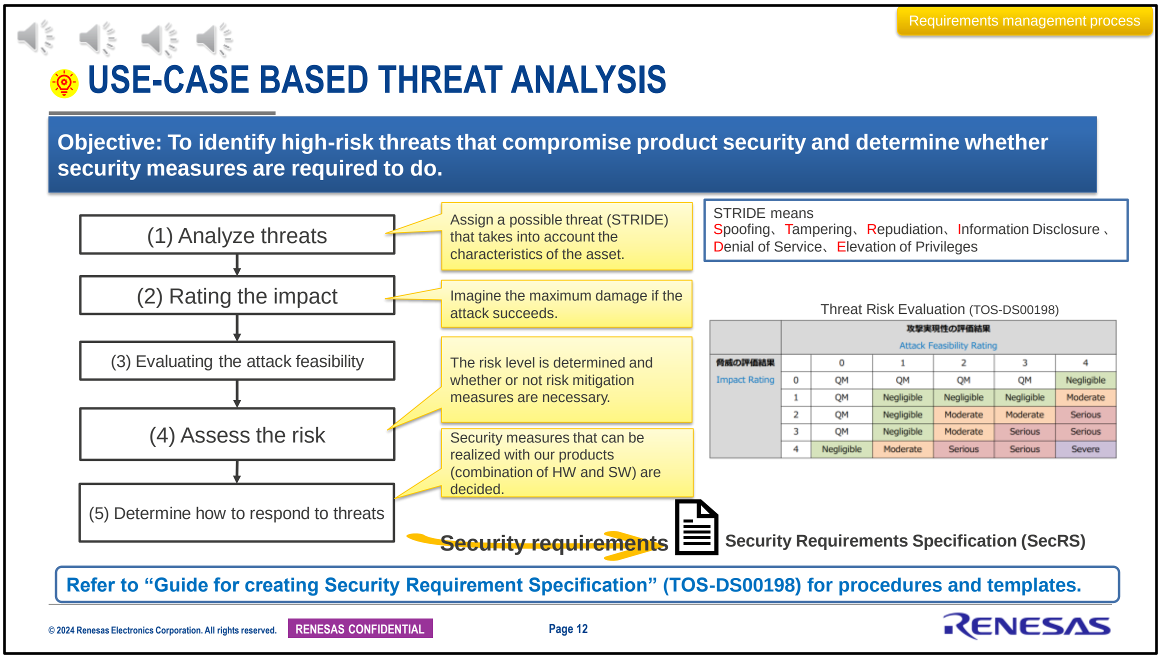
Market requirement, Customer requirement
Creating security context
Preconditions for product development such as internal structure of the product and environment where the product is used.
Security context
・System architecture diagram
・Life cycle list
・Prerequisite list
Deriving use case
Scenarios that shows how product to be used.
Use case
Creating data flow diagram
Diagram that represents data flow and trust boundaries
Data flow diagram
Create asset list
Deciding assets should be protected from threats.
Asset list
Use-case based threat analysis (Next page)
Attack list-based threat analysis (p14)
Creating security requirement

Refer to "Guide for creating Security Requirement Specification" (TOS-DS00198) for procedures and templates.

RENESAS CONFIDENTIAL Page 11

Security context.
The purpose of this activity is to determine the targets for threat analysis evaluation.
Create a security context using market and customer requirements as input.
This security context consists of the product's internal configuration, a system architecture diagram showing the external environment, a life cycle list from when the product is manufactured until it is disposed of, and a list of prerequisites such as the external environment when the product is used. It consists of them. Next, based on this context, we derive use cases, which are scenarios that show how the product is used.
Threat analysis is performed for this use case. Next, create a data flow diagram using the determined use case as input. Finally, from the data flow diagram created, determine which assets should be protected from threats. Assets to be protected can be functional data memory or the device itself.
We perform threat analysis and risk assessment using the created security context, and use case, etc. as input.

Procedures and formats to create the security context , refer to Security Requirements Specification Creation Guide, TOS-DS00198. It also shows the styles and examples of how to use them.



Requirements management process

USE-CASE BASED THREAT ANALYSIS

Objective: To identify high-risk threats that compromise product security and determine whether security measures are required to do.

(1) Analyze threats

Assign a possible threat (STRIDE) that takes into account the characteristics of the asset.

(2) Rating the impact

Imagine the maximum damage if the attack succeeds.

(3) Evaluating the attack feasibility

The risk level is determined and whether or not risk mitigation measures are necessary.

(4) Assess the risk

Security measures that can be realized with our products (combination of HW and SW) are decided.

(5) Determine how to respond to threats

Security requirements

Security Requirements Specification (SecRS)

STRIDE means
Spoofing、Tampering、Repudiation、Information Disclosure 、Denial of Service、Elevation of Privileges

Threat Risk Evaluation (TOS-DS00198)

		攻撃実現性の評価結果 Attack Feasibility Rating				
脅威の評価結果 Impact Rating		0	1	2	3	4
	0	QM	QM	QM	QM	Negligible
	1	QM	Negligible	Negligible	Negligible	Moderate
	2	QM	Negligible	Moderate	Moderate	Serious
	3	QM	Negligible	Moderate	Serious	Serious
	4	Negligible	Moderate	Serious	Serious	Severe

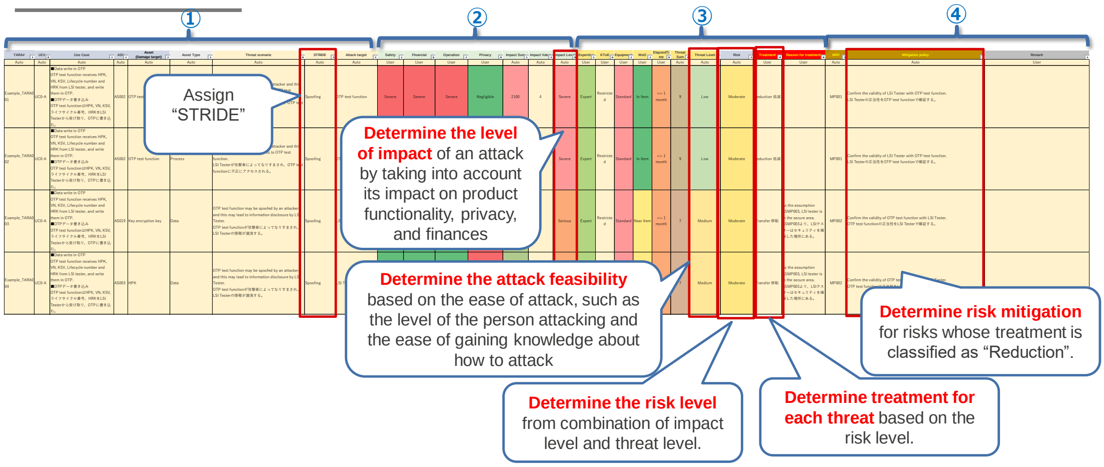
Refer to "Guide for creating Security Requirement Specification" (TOS-DS00198) for procedures and templates.

RENESAS CONFIDENTIAL Page 12 RENESAS

Threat analysis and risk assessment.
The purpose of this activity is to identify high-risk threats and determine whether security measures are required.
The rough steps are
1 to
5.
Create possible threat scenarios for use case. At this time, we analyze using stride as a guide word. Stride is an acronym for threat categories such as spoofing, tampering, and so on, as shown in the top right corner. For example, data in memory may be tampered with and information may be leaked. We derive scenarios in which tampering or information leaks occur and evaluate the damage that would be caused if such threats materialized. At this time, in addition to evaluating the impact, we also evaluate the feasibility of the attack. Based on the impact and feasibility of attacks evaluated in (2) and (3), we determine the risk level according to the colorfully colored table on the right. Based on the risk level determined in (4), the policy for handling the threat is determined.
ISO 21434 describes it as risk treatment. Specifically, we choose one

of four options: reduce risk, avoid it, transfer it, or retain it.
Determine mitigation strategies for the threats you determine to reduce risk.
For threat analysis and risk assessment procedures and formats, please refer to the Security Requirements Specification Creation Guide, TOS-DS00198.

EXAMPLE) USE-CASE BASED THREAT ANALYSIS



TARA#	UC#	Use Case	AS#	Asset (Damage target)	Asset Type	Threat scenario	STRIDE	Attack target
Auto	Auto	Auto	Auto	Auto	Auto	Auto	Auto	Auto
Example_TARA001	UC0-A	■Data write in OTP OTP test function receives HPK, VN, KSV, Lifecycle number and HRK from LSI tester, and write them in OTP. ■OTPデータ書き込み OTP test functionはHPK, VN, KSV, ライフサイクル番号、HRKをLSI Testerから受け取り、OTPに書き込む。	AS002	OTP test[illegible]	[illegible]	[illegible]ttacker and thi[illegible]OTP te[illegible]	Spoofing	OTP test function
Example_TARA002	UC0-A	■Data write in OTP OTP test function receives HPK, VN, KSV, Lifecycle number and HRK from LSI tester, and write them in OTP. ■OTPデータ書き込み OTP test functionはHPK, VN, KSV, ライフサイクル番号、HRKをLSI Testerから受け取り、OTPに書き込む。	AS002	OTP test function	Process	[illegible]ttacker and thi[illegible]ss to OTP test function. LSI Testerが攻撃者によってなりすまされ、OTP test functionに不正にアクセスされる。	Spoofing	[illegible]
Example_TARA003	UC0-A	■Data write in OTP OTP test function receives HPK, VN, KSV, Lifecycle number and HRK from LSI tester, and write them in OTP. ■OTPデータ書き込み OTP test functionはHPK, VN, KSV, ライフサイクル番号、HRKをLSI Testerから受け取り、OTPに書き込む。	AS019	Key encryption key	Data	OTP test function may be spoofed by an attacker and this may lead to information disclosure by LSI Tester. OTP test functionが攻撃者によってなりすまされ、LSI Testerの情報が漏洩する。	Spoofing	[illegible]
Example_TARA004	UC0-A	■Data write in OTP OTP test function receives HPK, VN, KSV, Lifecycle number and HRK from LSI tester, and write them in OTP. ■OTPデータ書き込み OTP test functionはHPK, VN, KSV, ライフサイクル番号、HRKをLSI Testerから受け取り、OTPに書き込む。	AS003	HPK	Data	OTP test function may be spoofed by an attacker and this may lead to information disclosure by LSI Tester. OTP test functionが攻撃者によってなりすまされ、LSI Testerの情報が漏洩する。	Spoofing	[illegible]

TARA#	Safety	Financial	Operation	Privacy	Impact Sum	Impact Value	Impact Level	Expertise	KToE	Equipment	WoO	ElapsedTime	Threat Sum	Threat Level	Risk	Treatment	Reason for treatment	MP#	Mitigation policy	Remark
Auto	User	User	User	User	Auto	Auto	Auto	User	User	User	User	User	Auto	Auto	Auto	User	User	Auto	Auto	User
Example_TARA001	Severe	Severe	Severe	Negligible	2100	4	Severe	Expert	Restricted	Standard	In Item	<= 1 month	9	Low	Moderate	eduction 低減		MP001	Confirm the validity of LSI Tester with OTP test function. LSI Testerの正当性をOTP test functionで確証する。	
Example_TARA002	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	Severe	Expert	Restricted	Standard	In Item	<= 1 month	9	Low	Moderate	eduction 低減		MP001	Confirm the validity of LSI Tester with OTP test function. LSI Testerの正当性をOTP test functionで確証する。	
Example_TARA003	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	Serious	Expert	Restricted	Standard	Near Item	<= 1 month	7	Medium	Moderate	ransfer 移転	s the assumption SMP003, LSI tester is n the secure area. SMP003より、LSIテスターはセキュリティを確保した場所にある。	MP002	Confirm the validity of OTP test function with LSI Tester. OTP test functionの正当性をLSI Testerで確証する。	
Example_TARA004	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	7	Medium	Moderate	ransfer 移転	s the assumption SMP003, LSI tester is n the secure area. SMP003より、LSIテスターはセキュリティを確保した場所にある。	MP002	Confirm the validity of OTP tes[illegible] Tester. OTP test fun[illegible]	

Assign "STRIDE"

Determine the level of impact of an attack by taking into account its impact on product functionality, privacy, and finances

Determine the attack feasibility based on the ease of attack, such as the level of the person attacking and the ease of gaining knowledge about how to attack

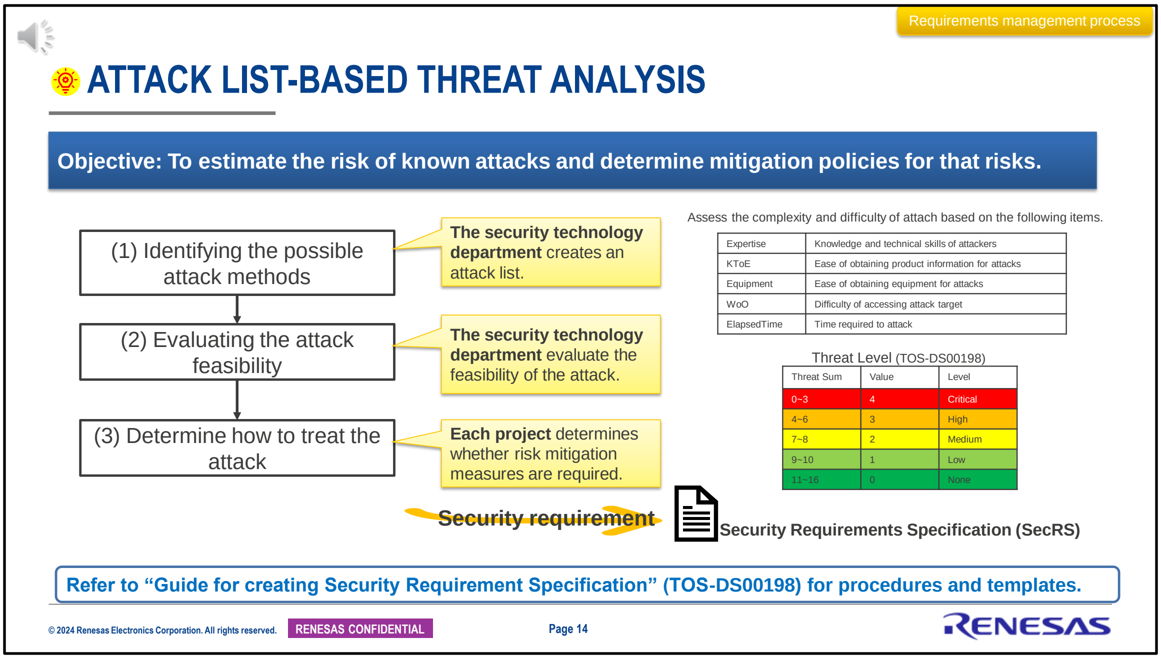
Determine the risk level from combination of impact level and threat level.

Determine treatment for each threat based on the risk level.

Determine risk mitigation for risks whose treatment is classified as "Reduction".

RENESAS CONFIDENTIAL

This is an example of creating TARA.
By using the form provided in TOS-DS00198 and filling it out from left to right, you can conduct a threat analysis and risk assessment by following the steps 1 to 5 described on the previous page.



Requirements management process

ATTACK LIST-BASED THREAT ANALYSIS

Objective: To estimate the risk of known attacks and determine mitigation policies for that risks.

(1) Identifying the possible attack methods

The security technology department creates an attack list.

(2) Evaluating the attack feasibility

The security technology department evaluate the feasibility of the attack.

(3) Determine how to treat the attack

Each project determines whether risk mitigation measures are required.

Security requirement

Assess the complexity and difficulty of attach based on the following items.

Expertise	Knowledge and technical skills of attackers
KToE	Ease of obtaining product information for attacks
Equipment	Ease of obtaining equipment for attacks
WoO	Difficulty of accessing attack target
ElapsedTime	Time required to attack

Threat Level (TOS-DS00198)

Threat Sum	Value	Level
0~3	4	Critical
4~6	3	High
7~8	2	Medium
9~10	1	Low
11~16	0	None

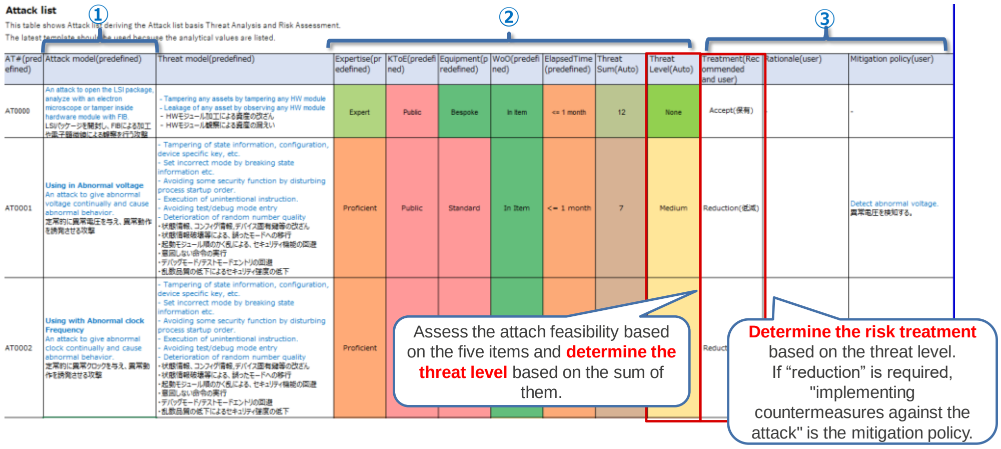
Security Requirements Specification (SecRS)

Refer to "Guide for creating Security Requirement Specification" (TOS-DS00198) for procedures and templates.

Attack list-based threat analysis.
The purpose of this attack list-based threat analysis is to estimate the risk to known attacks and determine mitigations for that risk.
The analysis flow is: First. Identifying the possible attack methods. Second. Evaluating the attack feasibility. Third, determine how to treat the attack.
While the previous threat analysis evaluated threats against a use case, this attack list-based threat analysis evaluates the feasibility of possible attack methods. The feasibility of an attack is evaluated from five perspectives, such as the attacker's technique and the time required for the attack, as described in top right table. Based on the evaluation results of the five items, the risk level is determined according to the bottom right table. If it is determined that risk reduction measures are necessary, those risk reduction measures become security requirements. Regarding attack list-based threat analysis, please refer to the Security Requirements Specification Creation Guide, TOS-DS00198, for procedures and formats.

Requirements management process

EXAMPLE) ATTACK LIST-BASED THREAT ANALYSIS



Attack list

This table shows Attack list deriving the Attack list basis Threat Analysis and Risk Assessment.
The latest template should be used because the analytical values are listed.

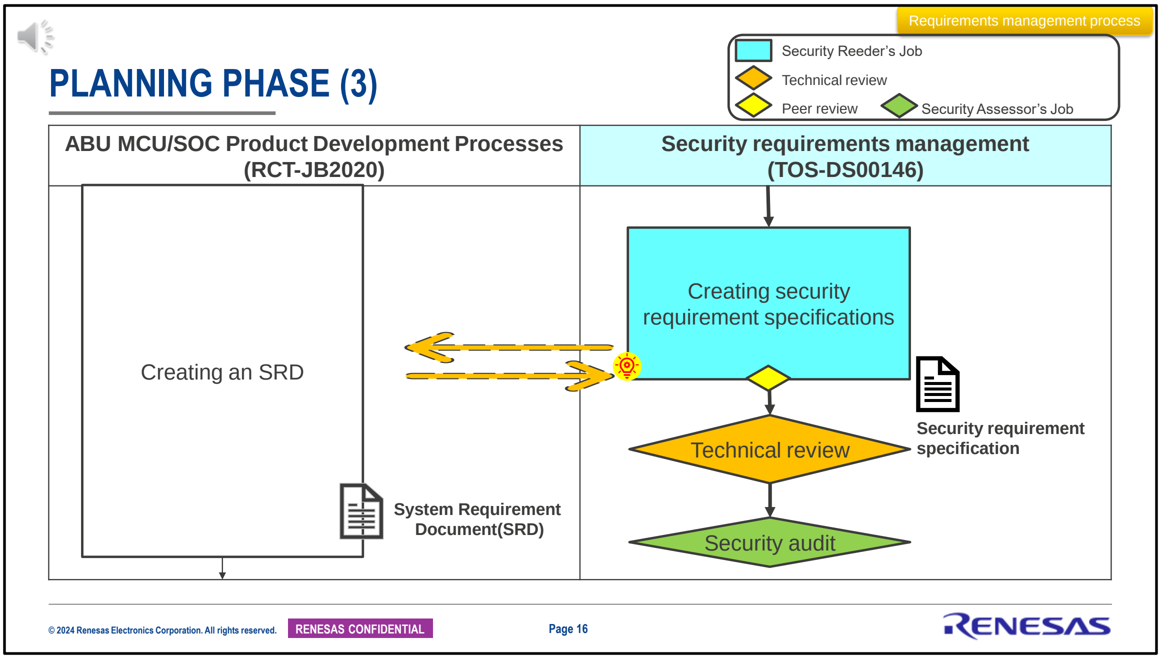
AT#(predefined)	Attack model(predefined)	Threat model(predefined)	Expertise(predefined)	KToE(predefined)	Equipment(predefined)	WoO(predefined)	ElapsedTime(predefined)	Threat Sum(Auto)	Threat Level(Auto)	Treatment(Recommended and user)	Rationale(user)	Mitigation policy(user)
AT0000	An attack to open the LSI package, analyze with an electron microscope or tamper inside hardware module with FIB. LSIパッケージを開封し、FIBによる加工や電子顕微鏡による観察を行う攻撃	- Tampering any assets by tampering any HW module - Leakage of any asset by observing any HW module - HWモジュール加工による資産の改ざん - HWモジュール観察による資産の漏えい	Expert	Public	Bespoke	In Item	<= 1 month	12	None	Accept(保有)	-	-
AT0001	**Using in Abnormal voltage** An attack to give abnormal voltage continually and cause abnormal behavior. 定常的に異常電圧を与え、異常動作を誘発させる攻撃	- Tampering of state information, configuration, device specific key, etc. - Set incorrect mode by breaking state information etc. - Avoiding some security function by disturbing process startup order. - Execution of unintentional instruction. - Avoiding test/debug mode entry - Deterioration of random number quality ・状態情報、コンフィグ情報,デバイス固有鍵等の改ざん ・状態情報破壊等による、誤ったモードへの移行 ・起動モジュール順のかく乱による、セキュリティ機能の回避 ・意図しない命令の実行 ・デバッグモード/テストモードエントリの回避 ・乱数品質の低下によるセキュリティ強度の低下	Proficient	Public	Standard	In Item	<= 1 month	7	Medium	Reduction(低減)		Detect abnormal voltage. 異常電圧を検知する。
AT0002	**Using with Abnormal clock Frequency** An attack to give abnormal clock continually and cause abnormal behavior. 定常的に異常クロックを与え、異常動作を誘発させる攻撃	- Tampering of state information, configuration, device specific key, etc. - Set incorrect mode by breaking state information etc. - Avoiding some security function by disturbing process startup order. - Execution of unintentional instruction. - Avoiding test/debug mode entry - Deterioration of random number quality ・状態情報、コンフィグ情報,デバイス固有鍵等の改ざん ・状態情報破壊等による、誤ったモードへの移行 ・起動モジュール順のかく乱による、セキュリティ機能の回避 ・意図しない命令の実行 ・デバッグモード/テストモードエントリの回避 ・乱数品質の低下によるセキュリティ強度の低下	Proficient							Reduct		

Assess the attach feasibility based on the five items and **determine the threat level** based on the sum of them.

Determine the risk treatment based on the threat level. If “reduction” is required, "implementing countermeasures against the attack" is the mitigation policy.

© 2024 Renesas Electronics Corporation. All rights reserved. RENESAS CONFIDENTIAL

This is an example of creating an attack list-based threat analysis. Perform the analysis using the form provided in TOS-DS00198. 1 and 2 have been analyzed by the security technology department, so each project decides how to handle risk in 3.



Requirements management process

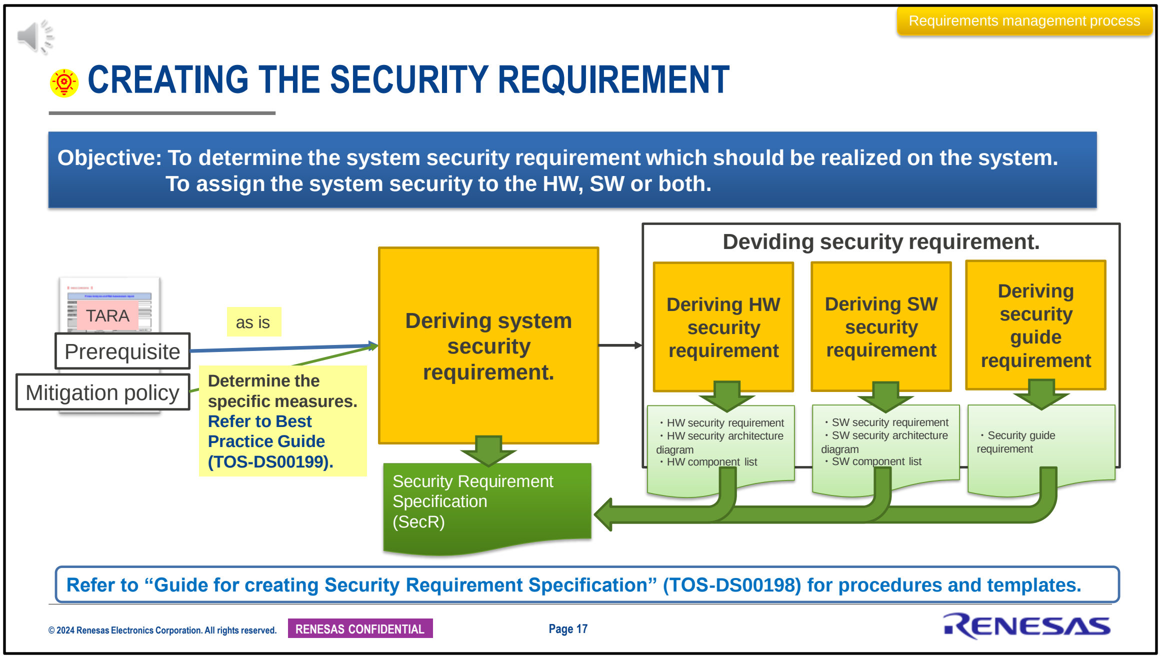
PLANNING PHASE (3)

🟦 Security Reeder’s Job
🔶 Technical review
◆ Peer review
◆ Security Assessor’s Job

ABU MCU/SOC Product Development Processes (RCT-JB2020)	Security requirements management (TOS-DS00146)
Creating an SRD System Requirement Document(SRD)	Creating security requirement specifications Security requirement specification Technical review Security audit

© 2024 Renesas Electronics Corporation. All rights reserved. RENESAS CONFIDENTIAL Page 16

Also, let's go back to explaining the development flow.
Earlier, I explained that TARA is implemented at the same time as the SRD is created. This is an explanation of the flow after implementing TARA.
According to RCT-JB2020, security requirements are determined based on the results of TARA during the time of creating the SRD. Then, a documented security requirements specification is output.
After a peer review is conducted on the created security requirements specification, a technical review is conducted. After the issues identified in the technical review have been addressed, a security assessor conducts a security audit.
The security audit is completed and the security requirements management process concludes.
The following pages describe security requirements.



Requirements management process

CREATING THE SECURITY REQUIREMENT

**Objective: To determine the system security requirement which should be realized on the system.
To assign the system security to the HW, SW or both.**

TARA

Prerequisite

Mitigation policy

as is

Determine the specific measures. Refer to Best Practice Guide (TOS-DS00199).

Deriving system security requirement.

Security Requirement Specification (SecR)

Deviding security requirement.

Deriving HW security requirement

- HW security requirement
- HW security architecture diagram
- HW component list

Deriving SW security requirement

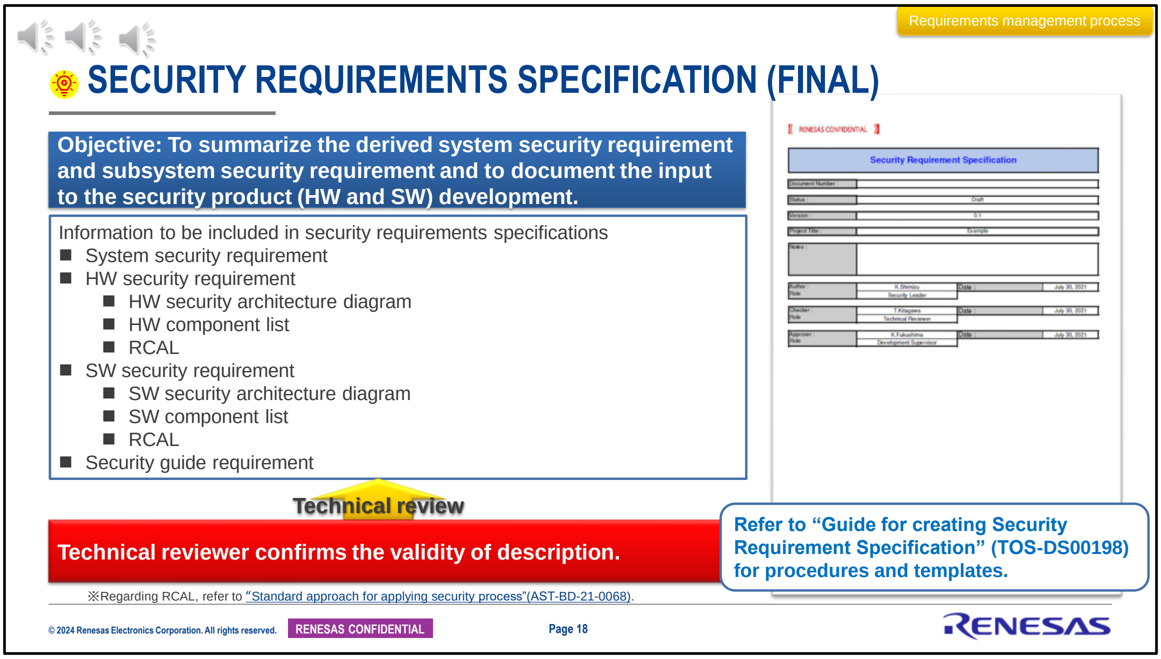
- SW security requirement
- SW security architecture diagram
- SW component list

Deriving security guide requirement

- Security guide requirement

Refer to "Guide for creating Security Requirement Specification" (TOS-DS00198) for procedures and templates.

Creating the security requirements.
The purpose is to determine all the risk reduction measures that should be implemented in the system as requirements for the system.
In order to achieve system security requirements, requirements must be assigned to the hardware, software, or both that make up the system.
System security requirements are determined from the prerequisites and the mitigation policy derived from Tara's results. Refer to best practices guides when determining specific mitigation strategies and developing system security requirements.
Next, divide the determined system security requirements into requirements for hardware, software, and security guides. Hardware security requirements serve as inputs for hardware development, and software security requirements serve as inputs for software development. Security guide requirements are requirements for customers or software developers and serve as input for creating security guides.
For procedures and formats, please refer to Security Requirements Specification Creation Guide, TOS-DS00198.



Requirements management process

SECURITY REQUIREMENTS SPECIFICATION (FINAL)

Objective: To summarize the derived system security requirement and subsystem security requirement and to document the input to the security product (HW and SW) development.

Information to be included in security requirements specifications

- System security requirement
- HW security requirement
  - HW security architecture diagram
  - HW component list
  - RCAL
- SW security requirement
  - SW security architecture diagram
  - SW component list
  - RCAL
- Security guide requirement

Technical review

Technical reviewer confirms the validity of description.

【 RENESAS CONFIDENTIAL 】

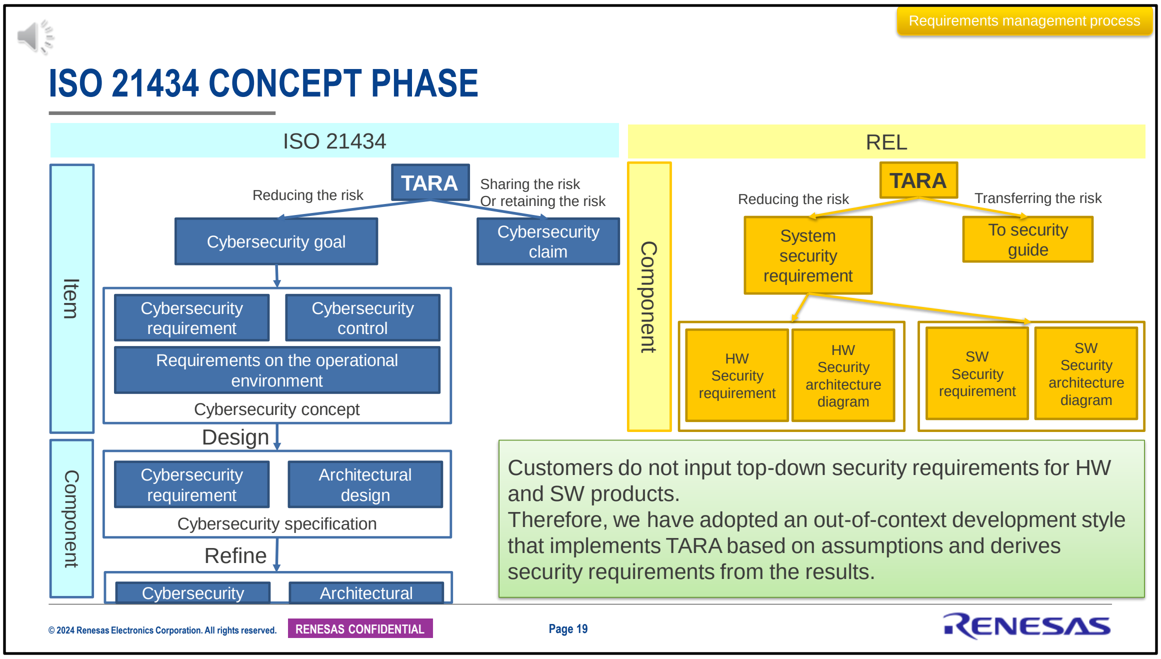
Security Requirement Specification

Document Number :			
Status :	Draft		
Version :	0.1		
Project Title :	Example		
Notes :			
Author : Role	K.Shimizu Security Leader	Date :	July 30, 2021
Checker : Role	T.Kitagawa Technical Reviewer	Date :	July 30, 2021
Approver : Role	K.Fukushima Development Supervisor	Date :	July 30, 2021

Refer to "Guide for creating Security Requirement Specification" (TOS-DS00198) for procedures and templates.

※Regarding RCAL, refer to "Standard approach for applying security process"(AST-BD-21-0068).

Security requirements specification.
A security requirements specification is a document that summarizes the system security requirements, hardware security requirements, software security requirements, and security guide requirements as explained on the previous page.
The information described in the security requirements specification includes system security requirements, etc.
It looks like this.
Here we have something called R-cal. It is an abbreviation for Renesas Cybersecurity Assurance Level, and each hardware and software component is classified from R-cal1 to R-cal 3 depending on the cybersecurity risk. 3 is the highest risk and requires a full security development process. For more information, please refer to the Standard Approach for Applying Security Process on the Cybersecurity website.
After peer review, the created security requirements specification is reviewed by a technical reviewer to confirm the validity of the content.
For procedures and formats, please refer to Security Requirements Specification Creation Guide, TOS-DS00198.



Requirements management process

ISO 21434 CONCEPT PHASE

ISO 21434

Item

TARA

Reducing the risk

Sharing the risk
Or retaining the risk

Cybersecurity goal

Cybersecurity claim

Cybersecurity requirement

Cybersecurity control

Requirements on the operational environment

Cybersecurity concept

Design

Component

Cybersecurity requirement

Architectural design

Cybersecurity specification

Refine

Cybersecurity

Architectural

REL

Component

TARA

Reducing the risk

Transferring the risk

System security requirement

To security guide

HW Security requirement

HW Security architecture diagram

SW Security requirement

SW Security architecture diagram

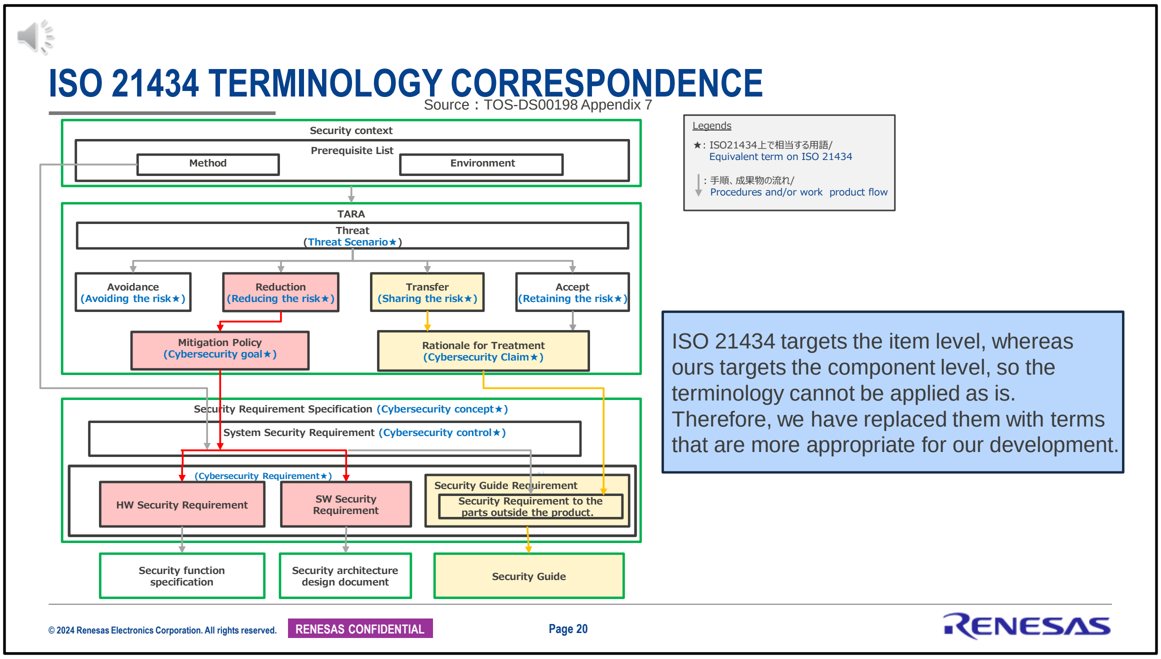
Customers do not input top-down security requirements for HW and SW products.
Therefore, we have adopted an out-of-context development style that implements TARA based on assumptions and derives security requirements from the results.

RENESAS CONFIDENTIAL

Page 19

ISO 21434, concept phase.
On the left, you will find an overview of ISO 21434 Chapter 9 Concept Phase.
Conduct TARA at item level. Then, identify the risks and decide on treatments for those risks. Cybersecurity goals are set when reducing risk. Cybersecurity claims are set up when risks are shared or retained.
To achieve cybersecurity goals, a cybersecurity concept is created that includes cybersecurity requirements. This cybersecurity requirement is assigned to the component. Cybersecurity requirements are then subdivided and assigned to the components or modules that make up the components.
In this way, in ISO 21434, security requirements come down from the top. In contrast, the MCU and S O C developed by our company are developed for general-purpose use, so there are no requirements for our products from specific customers. We do what ISO 21434 does at the item level at the component level, and derive and develop requirements ourselves.
Although it does not completely match the terminology proposed in ISO 21434, we have constructed a requirements derivation process

based on a similar idea.
I will explain it in detail in the next slide.



ISO 21434 TERMINOLOGY CORRESPONDENCE

Source：TOS-DS00198 Appendix 7

Security context

Prerequisite List

Method

Environment

TARA

Threat (Threat Scenario★)

Avoidance (Avoiding the risk★)

Reduction (Reducing the risk★)

Transfer (Sharing the risk★)

Accept (Retaining the risk★)

Mitigation Policy (Cybersecurity goal★)

Rationale for Treatment (Cybersecurity Claim★)

Security Requirement Specification (Cybersecurity concept★)

System Security Requirement (Cybersecurity control★)

(Cybersecurity Requirement★)

HW Security Requirement

SW Security Requirement

Security Guide Requirement

Security Requirement to the parts outside the product.

Security function specification

Security architecture design document

Security Guide

Legends

★: ISO21434上で相当する用語/ Equivalent term on ISO 21434

↓: 手順、成果物の流れ/ Procedures and/or work product flow

ISO 21434 targets the item level, whereas ours targets the component level, so the terminology cannot be applied as is. Therefore, we have replaced them with terms that are more appropriate for our development.

RENESAS CONFIDENTIAL

Page 20

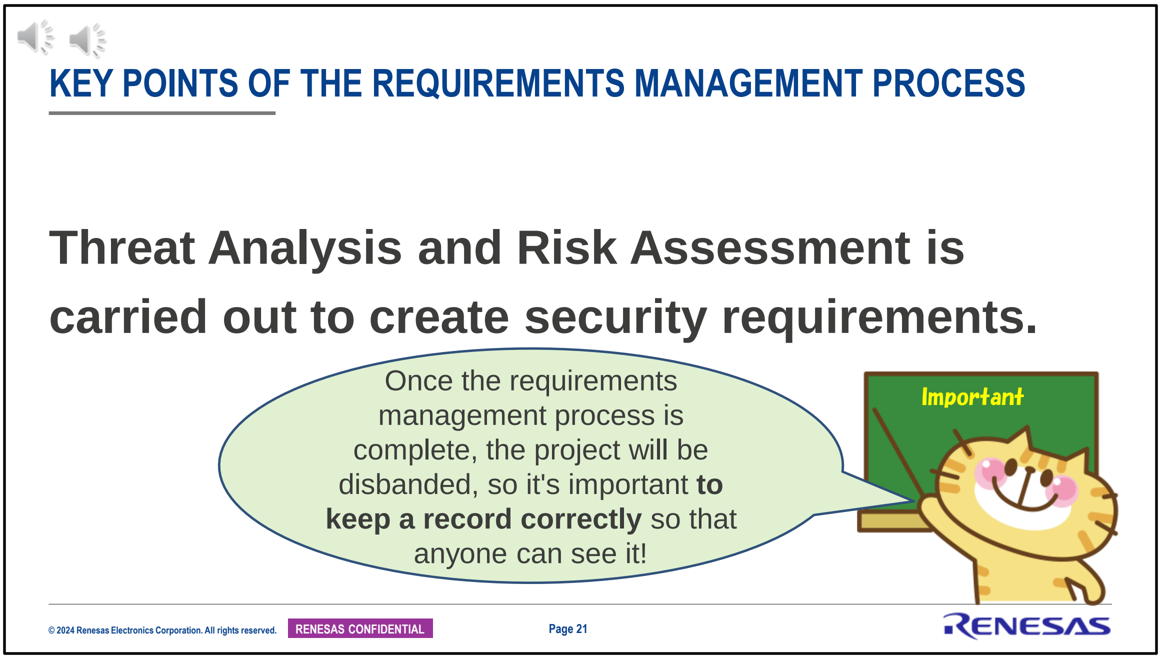
RENESAS

ISO 21434, terminology correspondence.
This diagram shows the correspondence between the terms used mainly in Chapter 9 Concept Phase of ISO 21434 and the terms used by our company.
This is specified in TOS-DS00198 Appendix 7.

The flow of security requirements derivation is shown in red. As a result of threat analysis, we define risk mitigation policy as hardware and software security requirements for threats that are determined to reduce risks.
This flow is in line with ISO 21434.
The yellow color indicates how cybersecurity claims are handled. As a result of threat analysis, we include the rationale for determining risk transfer in our security guide and disclose it to our customers. By doing so, customers who adopt our products developed out of context can verify the validity of their cybersecurity claims. This would meet the requirements of ISO 21434 RQ-06-20.

As shown here, the concept phase of ISO 21434 uses terminology with

an item level in mind, so for our company, which develops semiconductor products, there are some terms that we cannot use as intended. Therefore, for example, we are changing the reading to use Transfer instead of Sharing the risk.
Before coordinating with customers, please read the explanation of TOS-DS00198 once to avoid any discrepancies in the use of ISO 21434 terminology.



KEY POINTS OF THE REQUIREMENTS MANAGEMENT PROCESS

Threat Analysis and Risk Assessment is carried out to create security requirements.

Once the requirements management process is complete, the project will be disbanded, so it's important **to keep a record correctly** so that anyone can see it!

RENESAS CONFIDENTIAL Page 21 RENESAS

Key points of the requirements management process.
The requirements management process involves performing threat analysis and risk assessment, and creating security requirements. The security requirements output from the requirements management process serve as input for hardware and software development. Even if a requirements management project is disbanded, it is important to keep accurate records so that hardware and software developers can understand why certain security requirements were decided upon.

This concludes our explanation of the requirements management process. Thank you for your viewing.